The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
https://www.us-cert.gov/tlp/

DATE(S) ISSUED:
09/09/2020

SUBJECT:
Multiple Vulnerabilities in Adobe InDesign, Adobe Framemaker, and Adobe Experience Manager Could Allow for Arbitrary Code Execution (APSB20-52, APSB20-54, APSB20-56)

OVERVIEW:
Multiple vulnerabilities have been discovered in Adobe InDesign, Adobe Framemaker, and Adobe Experience Manager, the most severe of which could allow for arbitrary code execution. Adobe InDesign is a desktop publishing and typesetting software that can be used to create works such as posters, flyers, brochures, magazines, newspapers, presentations, books and ebooks. Adobe FrameMaker is a document processor designed for writing and editing large or complex documents, including structured documents. Adobe Experience Manager (AEM), is a comprehensive content management solution for building websites, mobile apps and forms. Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
There are no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Adobe InDesign 15.1.2 and earlier versions
- Adobe Framemaker 2019.0.6 and earlier versions
- Adobe Experience Manager 6.5.5.0 and earlier versions
- Adobe Experience Manager 6.4.8.1 and earlier versions
- Adobe Experience Manager 6.3.3.8 and earlier versions
- Adobe Experience Manager 6.2 SP1-CFP20 and earlier versions
- AEM Forms add-on Pack 5 and earlier versions

RISK:
Government:

- Large and medium government entities: **Low**

- Small government entities: **Low**

Businesses:

- Large and medium business entities: **Low**
- Small business entities: **Low**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Adobe InDesign, Adobe Framemaker, and Adobe Experience Manager the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

- Adobe InDesign has five memory corruption vulnerabilities that could lead to arbitrary code execution. (CVE-2020-9727, CVE-2020-9728, CVE-2020-9729, CVE-2020-9730, CVE-2020-9731)
- Adobe Framemaker has one stack-based buffer overflow vulnerabilities that could lead to arbitrary code execution. (CVE-2020-9725)
- Adobe Framemaker has one out-of-bounds read vulnerability that could lead to arbitrary code execution. (CVE-2020-9726)
- Adobe Experience Manager nine arbitrary javaScript execution in the browser vulnerabilities that could lead to stored cross-site scripting. (CVE-2020-9732, CVE-2020-9734, CVE-2020-9735, CVE-2020-9736, CVE-2020-9737, CVE-2020-9738, CVE-2020-9740, CVE-2020-9741, CVE-2020-9742)
- Adobe Experience Manager has one execution with unnecessary privileges vulnerability that could cause sensitive information disclosure (CVE-2020-9733)
- Adobe Experience Manager has one HTML injection vulnerability that could lead to arbitrary HTML injection in the browser (CVE-2020-9743)

Successful exploitation of the most severe of these vulnerabilities could result in arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this application has been configured to have fewer user rights on the system, exploitation of the most severe of these vulnerabilities could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services

REFERENCES:

Adobe:

https://helpx.adobe.com/security/products/indesign/apsb20-52.html
https://helpx.adobe.com/security/products/framemaker/apsb20-54.html
https://helpx.adobe.com/security/products/experience-manager/apsb20-56.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9725
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9726
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9727
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9728
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9729
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9730
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9731
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9732
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9733
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9734
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9735
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9736
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9737
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9738
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9740
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9741
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9742
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9743